Possiblistic Security and the Refinement Paradox

By: David Bibighaus

15 March 04

Secure State Proofs

- Construct an Access Control Matrix
  - Specifies the set of allowed accesses
- Construct a transformation function
- The system is secure if you can prove…
  - It starts in a secure state
  - Applying the transformation function keeps the system in secure state.

Visualization of These Proofs

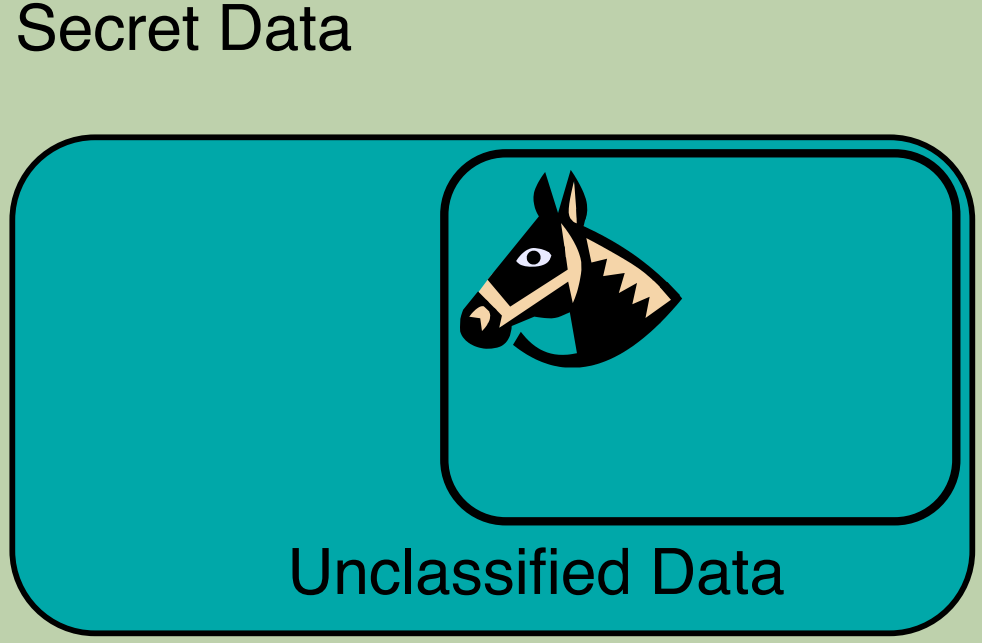
Secret Data

Unclassified Data

- Horse Starts In Fence
- Horse Can't Jump Fence

- Horse will stay in Fence

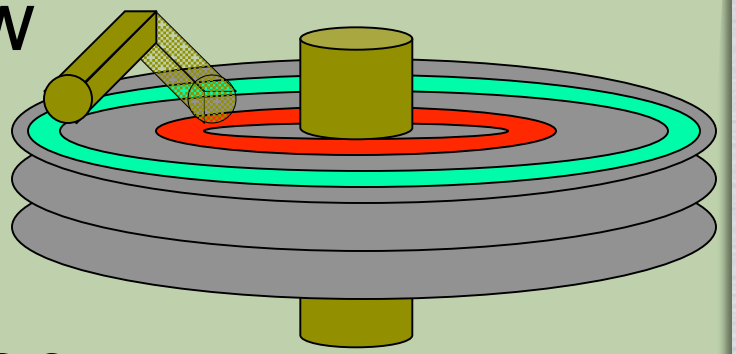
Refinement



- Further restrict where the horse can roam
- Access is a subset of the original
- Example: DAC
- Does not impact the security of the system

…the Rest of the Story.

- Disk Arm
- Low Process reads low document
- High reads high
- BUT the implementation causes the disk arm to move.

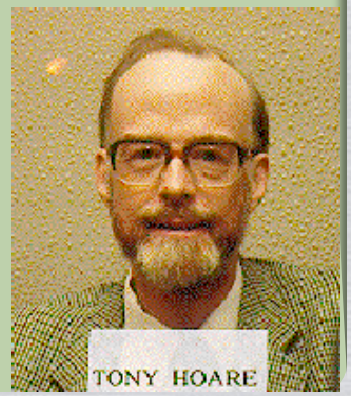


Hidden Channels

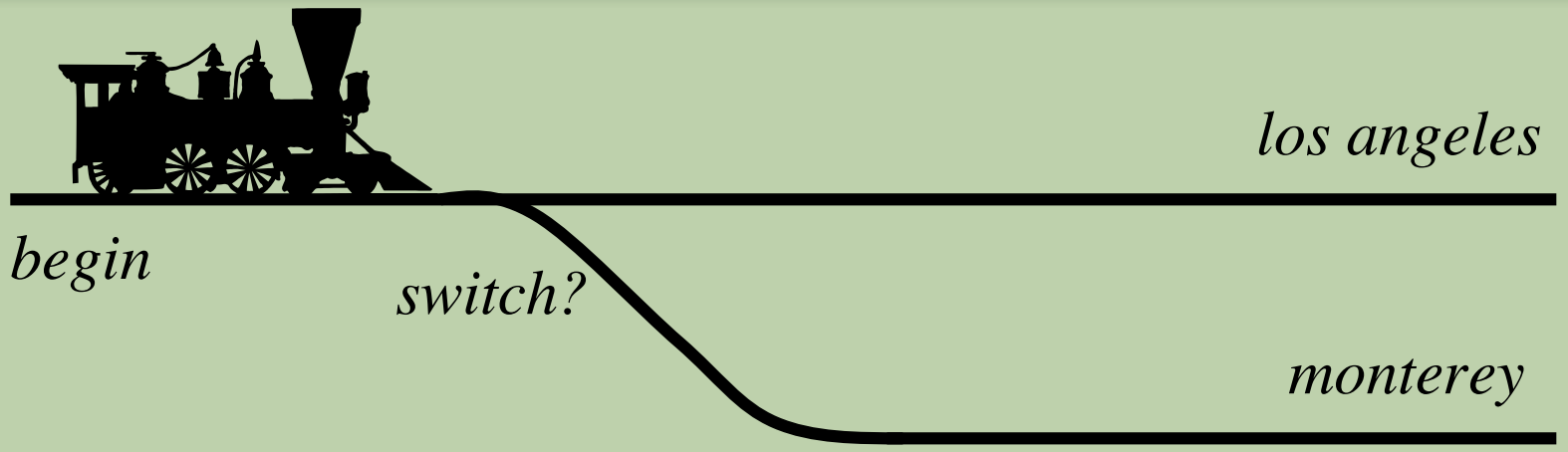
- Information is communicated without reading And writing
- How do you fix it?
  - Change the definition of reading and writing (But how do you know if you are right?)
  - Change the security property (Redefine what it means to be secure).

Communicating Sequential Processes (CSP)

- Developed by Tony Hoare
- One of two competing process Algebras
- Mathematical logic for describing systems.
- 3rd Most Cited Work In Computer Science

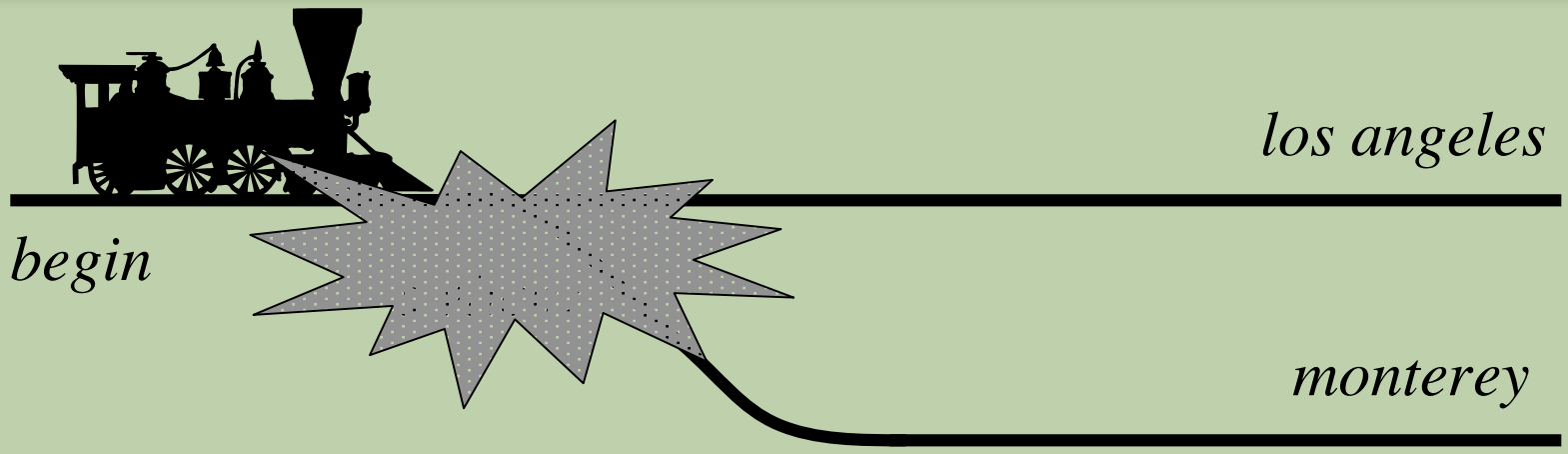


Train Example



TRAIN = $(b \blacklozenge l) \mid (b \blacklozenge s \blacklozenge m)$

Train with Concealment



TRAIN\{s} = (b ♦ l) Û (b ♦ m)

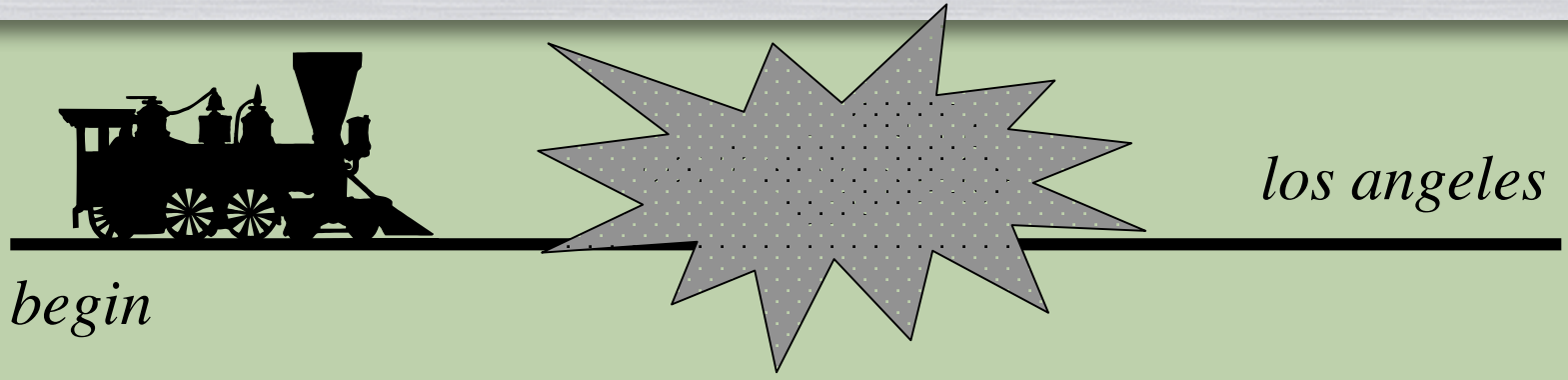
2nd Train Example

car?

los angeles

begin

2nd Train with Concealment



TRAIN\{c} = b ♦ l

Security

- Divide events into high security and low security.
- Show that from low's point of view, the system behaves the same weather or not the high events took place.
- Formally

  Noninterference $\Leftrightarrow$

  $$P\backslash\{high\} = P||STOP_{high}$$

NonInterference

- Don't care about defining reading or writing
  - No hidden channels (we think).
- A system is secure when high security events cannot affect (interfere) with the behavior of a low security process.

Noninterference $\Leftrightarrow$

$P\backslash\{high\} = P||STOP_{high}$

…the Rest of the Story

- Consider the following problem

P = $(a \blacklozenge x \blacklozenge b \blacklozenge z) \mid$

$(a \blacklozenge b) \mid$

$(c \blacklozenge w \blacklozenge d \blacklozenge y) \mid$

$(c \blacklozenge d)$

…the Rest of the Story

- This is a refinement (subset) of the original

P2 = $(a \blacklozenge x \blacklozenge b \blacklozenge z) \mid$

$(a \blacklozenge b) \mid$

$(c \blacklozenge w \blacklozenge d \blacklozenge y) \mid$

~~$(c \blacklozenge d)$~~

Where we stand now

- Secure State Proofs
  - Secure Refinements
  - Hidden Channels
- NonInterference Proofs
  - No Hidden Channels
  - No Secure Refinements